

KAMIE F. BROWN (8520)
KRISTINA M. DUBOIS (18908)
RAY QUINNEY & NEBEKER P.C.
36 South State Street, Suite 1400
P. O. Box 45385
Salt Lake City, UT 84145-0385
Tel: (801) 532-1500
Fax: (801) 532-7543
kbrown@rqn.com
kdubois@rqn.com

JUSTIN J. BORON (*pro hac vice forthcoming*)
KEVIN M. RINGEL (*pro hac vice forthcoming*)
FREEMAN MATHIS & GARY, LLP
1600 Market Street
Philadelphia, PA 19103-7240
Tel: (215) 789-4919
justin.boron@fmglaw.com
kevin.ringel@fmglaw.com

Attorneys for Academy Mortgage Corporation

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION**

LISA KUCHERRY, on behalf of herself
and all others similarly situated,

Plaintiff,

v.

ACADEMY MORTGAGE CORPORATION,

Defendant.

**DEFENDANT’S MOTION TO DISMISS
PLAINTIFF’S COMPLAINT**

Case No. 2:24-cv-00078-TC-CMR

Judge Tena Campbell

Magistrate Judge Cecilia M. Romero

Defendant Academy Mortgage Corporation (“AMC”) moves to dismiss Plaintiff’s Proposed Class Action Complaint. Plaintiff lacks standing and has failed to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6).

SPECIFIC RELIEF SOUGHT AND GROUNDS FOR RELIEF

This case arises from a data security incident that occurred when a third-party hacker launched a cyberattack on AMC’s data security system. Plaintiff is a customer of AMC and attempts to bring this claim on behalf of herself and a putative class (the “Putative Class”).¹ Plaintiff asserts five claims including: (1) negligence, (2) negligence *per se*, (3) breach of implied contract, (4) invasion of privacy, and (5) unjust enrichment. Plaintiff’s claims are unsupported and should be summarily dismissed.

First, Plaintiff’s Complaint should be dismissed for lack of Article III standing. As succinctly stated by the U.S. Supreme Court in *TransUnion LLC v. Ramirez*, “[n]o concrete harm, no standing.” 594 U.S. 413, 417, 442 (2021). Plaintiff’s Proposed Class Action Complaint must be dismissed as Plaintiff alleges no harm or loss that satisfies her constitutional burden to plead an injury-in-fact traceable to the “data breach” event of which she complains. Specifically, Plaintiff does not allege any financial losses or actual misuse of her personal identification information (“PII”) caused by the March 2023 cybersecurity incident (the “Incident”). Instead, she relies on generalities about broad problems with data breaches, what happened to her around the same time as the Incident, conjectural future injuries, and efforts she took unnecessarily to mitigate against a hypothetical threat of future harm.

Second, even assuming Plaintiff has Article III standing to bring her claims, all counts of Plaintiff’s Complaint must be dismissed pursuant to Rule 12(b)(6). Plaintiff has not alleged an injury or damage for which the law recognizes a cause of action.

Therefore, AMC’s Motion to Dismiss should be granted with prejudice.

¹ References to “Plaintiff” include both the Plaintiff and the Putative Class.

ALLEGED FACTS

At the time of the incident in question, Defendant AMC was a privately held Utah-based mortgage lender serving customers across over 200 branches nationwide.² In March 2023, AMC was the victim of a criminal hack into part of its digital files. When AMC discovered unauthorized activity on its system, AMC immediately began containment, mitigation, and restoration efforts to terminate the activity and secure its network systems and data. In fact, AMC not only did what it should, it did more than what was legally required to protect its customers and employees. AMC notified approximately 284,000 customers and employees whose PII might have been accessible to the hacker. AMC also offered them free credit monitoring.

Plaintiff Lisa Kucherry is a former AMC customer whom AMC notified and to whom AMC offered free credit monitoring. Plaintiff alleges that as a condition of receiving mortgage services from AMC, Plaintiff provided AMC with her PII, including, but not limited to, her name and Social Security number. Proposed Class Action Complaint (“Complaint”), Dkt. #1, ¶ 24. On March 21, 2023, AMC experienced a network security incident by a criminal threat actor. *Id.* ¶ 28. Plaintiff contends that AMC failed to implement reasonable cybersecurity safeguards or policies to protect PII and stop breaches of its system, and, as a result, the security of Plaintiff’s PII was compromised. *Id.* ¶¶ 7, 9, 32, 35.

That is not the case. To the contrary, AMC underwent a complete forensic investigation which found no evidence that any sensitive information, including PII, had been misused.

² AMC’s assets (but not liabilities) were acquired by Guild Mortgage on or about February 13, 2024.

Regardless, out of an abundance of caution, on or about December 20, 2023, AMC issued a notice letter to certain potentially affected individuals. *Id.* ¶ 28.

Plaintiff specifically alleges that she provided AMC with her PII, including but not limited to her name and Social Security number, in order for Plaintiff to obtain AMC's mortgage services. *Id.* ¶ 24. Plaintiff contends that her identity is now at risk because her PII is "now in the hands of data thieves." *Id.* ¶ 10. She further alleges that Plaintiff has "experienc[ed] an increase in spam calls, texts, and/or emails, which upon information and belief, was caused by the Data Breach." *Id.* ¶ 141. She contends that, as a result of the data breach, she must conduct "constant surveillance of [her] financial and personal records, monitoring, and loss of rights," *id.* ¶ 57, 73, 126, an injury in the form of damages to and diminution in the value of her PII "in both legitimate and dark markets," *id.* ¶ 123, and that she has "spent time and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, researching online how to protect [herself] from fraud and identity theft, signing up for the credit monitoring and identity theft insurance services offered by Defendant, contacting law enforcement regarding suspicious calls, and monitoring [her] financial accounts for any indication of fraudulent activity, which may take years to detect." *Id.* ¶ 114. Plaintiff also alleges that the "Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence." *Id.* ¶ 142.

Plaintiff asserts five causes of action against AMC. The First Cause of Action, Negligence, alleges that Plaintiff entrusted her PII to AMC on the premise and with the understanding that AMC would safeguard her PII, use her PII for business purposes only, and/or not disclose her PII

to unauthorized third parties. *Id.* ¶¶ 27, 165. Plaintiff also alleges that AMC owed a duty to Plaintiff to employ reasonable data security measures in accordance with industry standards for data security and to exercise reasonable care in handling and using the PII in its care and custody. *Id.* ¶¶ 167-170. Plaintiff alleges AMC breached its duties by failing to exercise reasonable care in handling and securing the PII of Plaintiff which actually and proximately caused the Incident and Plaintiff's injuries. *Id.* ¶¶ 177, 194.

Plaintiff's Second Cause of Action, Negligence *Per Se*, based on the same facts as Count I, alleges that by failing to fully protect Plaintiff's PII from cybercriminals, AMC violated Section 5 of the Federal Trade Commission Act ("FTC Act"). *Id.* ¶ 198.

Plaintiff's Third Cause of Action, Breach of Implied Contract, also based on the same facts as Count I, alleges that AMC and Plaintiff entered into implied contracts whereby AMC "agreed to safeguard and protect" her PII "and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen." *Id.* ¶ 208.

Plaintiff's Fourth Cause of Action, Invasion of Privacy, alleges that Plaintiff had a reasonable expectation of privacy under Utah common law regarding her highly sensitive and confidential PII and was entitled to the protection of this information against disclosure to unauthorized third parties. *Id.* ¶¶ 226-228. Plaintiff further alleges that AMC's mishandling and disclosure of PII would be highly offensive and objectionable to a reasonable person. *Id.* ¶ 232. Plaintiff seeks injunctive relief and compensatory damages for the alleged invasion of privacy.

Plaintiff's Fifth Cause of Action, Unjust Enrichment, based on the same facts as Count III, alleges that Plaintiff "conferred a monetary benefit on Defendant" in the form of payment for the servicing of their mortgages and loans. *Id.* ¶ 236. Plaintiff further alleges that AMC should

disgorge all profits, benefits, and other compensation through a constructive trust because Plaintiff and Class Members may not have an adequate remedy at law. *Id.* ¶¶ 244-245.

All of Plaintiff's claims should be dismissed. Of paramount importance here, Plaintiff does not allege any identity theft or fraud as a result of the Incident. She is only able to point to a risk that her PII "is now in the hands of data thieves" who "can in the future commit a variety of crimes." *Id.* ¶¶ 10-11. Significantly, Plaintiff does not allege any fraudulent charges to her financial accounts, any fraudulent opening of credit cards or investment accounts in her name, or any unauthorized access to any of her other financial accounts. Other than the questionable "increase in spam calls," there are no allegations that Plaintiff's PII has been posted to the dark web as a result of the Incident. *Id.* ¶¶ 6, 141, 193, 243. To date, there has been no indication—and Plaintiff has not alleged—that Plaintiff's sensitive information has been misused or that Plaintiff has experienced identity theft or fraud. Instead, Plaintiff's contentions are based on the risk of future harm, *i.e.*, that she might experience identity theft or fraud in the indefinite future. This is insufficient to survive AMC's Motion to Dismiss.

STANDARD OF REVIEW

A motion to dismiss "under Rule 12(b)(6) tests the legal sufficiency of the claims asserted in a plaintiff's complaint." *Braun v. United States*, No.1:22-cv-00108-RJS-CMR, 2023 WL 6158943, at *4 (D. Utah Sept. 21, 2023) (unpublished). To survive dismissal under Rule 12(b)(6), a complaint must allege "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A complaint must contain "more than labels and conclusions" or "a formulaic recitation of the elements of a cause of action." *Bell Atlantic Corp.*

v. Twombly, 550 U.S. 544, 555 (2007). “Factual allegations must be enough to raise a right to relief above the speculative level.” *Id.* “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.*

ARGUMENT

I. PLAINTIFF LACKS STANDING UNDER ARTICLE III TO BRING THIS ACTION BECAUSE SHE HAS NOT ALLEGED THAT SHE HAS SUFFERED INJURY IN FACT.

A. *TransUnion’s* Sea Change To the Article III Standing Requirement.

“To satisfy Article III’s standing requirements, a plaintiff must show (1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Utah Physicians for a Healthy Env’t, Inc. v. TAP Worldwide, LLC*, 582 F. Supp. 3d, 881, 891 (D. Utah 2022) (quoting *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000)), *motion to certify appeal denied*, No. 2:19-CV-00628-DBB, 2022 WL 787972 (D. Utah Mar. 15, 2022) (unpublished). “For traceability, [a plaintiff] must demonstrate a connection between their purported injury and [the defendant’s] actions.” *Alfwear, Inc. v. IBKUL Corp.*, 672 F. Supp. 3d 1174, 1184 (D. Utah 2023).

“‘Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy’ under Article III” *Barrett v. Vivint, Inc.*, No. 2:19-cv-00568-DBB-CMR, 2020 WL 2558231, at *3 (D. Utah May 20, 2020) (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016)) (unpublished). “The Tenth Circuit ‘has repeatedly characterized standing as an element of subject matter jurisdiction’ and has held ‘that a dismissal for lack of standing can be at least

colorably characterized as a dismissal for lack of subject matter jurisdiction.” *Id.* (quoting *Hill v. Vanderbilt Capital Advisors, LLC*, 702 F.3d 1220, 1225 (10th Cir. 2012)). “When reviewing a factual attack on subject matter jurisdiction, a district court may not presume the truthfulness of the complaint’s factual allegations.” *Id.* (citing *Holt v. United States*, 46 F.3d 1000, 1003 (10th Cir. 1995)). At the pleading stage, a “plaintiff must ‘clearly . . . allege facts demonstrating each element.’” *Id.* (alteration in original) (quoting *Spokeo*, 136 S. Ct. at 1547).

In *TransUnion*, a class of individuals sued a credit reporting agency, under the Fair Credit Reporting Act, for failing “to use reasonable procedures to ensure the accuracy of their credit files.” 594 U.S. at 417. The Supreme Court concluded that 1,853 of the class members had standing, *i.e.*, they suffered “concrete reputational harm,” because the agency provided their credit reports to third parties and that the reports wrongfully indicated that the persons had a name that potentially matched names on a list maintained by the U.S. Treasury Department’s Office of Foreign Assets Control for known or suspected terrorists, drug traffickers, and other such criminals. *Id.* at 417, 432. Yet, the Supreme Court also concluded that the remainder of the class members were unable to demonstrate that they suffered concrete harm because their credit reports were not provided to any third-party. *Id.* at 417. As a result, those class members failed to show that they “suffered an injury in fact that is concrete, particularized, and actual or imminent.” *Id.* at 423.

In correcting misunderstandings about *Spokeo v. Robins*, 578 U.S. 330 (2016), the Supreme Court clarified that the decision was “not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal court.” *Id.* at 424-25. The Supreme Court also explained that the material risk of future

harm, without more, is not concrete harm and, in turn, does not confer standing— this is especially so where the risk of future harm has not materialized via a showing that the plaintiffs “were independently harmed by their exposure to the risk itself.” *Id.* at 436-38 (“The plaintiffs claimed that TransUnion could have divulged their misleading credit information to a third party at any moment. But the plaintiffs did not demonstrate a sufficient likelihood that their individual credit information would be requested by third-party businesses and provided by TransUnion during the relevant time period.”).

B. Courts Within the Tenth Circuit Have Repeatedly Held the Risk That Fraud or Identity Theft May Occur in the Future Cannot Support Standing for a Damages Claim.

While the Tenth Circuit has not yet addressed the question of whether the mere fact that a data breach occurred necessarily means that a customer has suffered a concrete injury, District Courts within the Tenth Circuit have resoundingly held, in cases with nearly identical fact patterns to the present case, that there is no concrete injury in this scenario.

In *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985 (W.D. Okla. Dec. 6 2021), this question was squarely addressed. The plaintiff in *Legg*, like Plaintiff here, did not allege that any misuse of the data occurred. 574 F. Supp. 3d at 993. In denying the plaintiff’s standing, the *Legg* court stated that damages based not on any actual fraud or identity theft that occurred as a result of the data breach, but on the risk that fraud or identity theft may occur in the future, cannot support standing for a damages claim. *Id.* Like Plaintiff’s claim of an increase in “spam calls,” the closest the *Legg* plaintiff came to “alleging misuse is a statement that there has been a ‘dramatic increase in the amount and frequency of phishing emails she has been receiving over the last few months.’” *Id.* However, “the receipt of phishing emails, while perhaps ‘consistent with’ data misuse, does

not ‘plausibly suggest’ that any actual misuse of Plaintiff’s personal identifying information has occurred.” *Id.* (quoting *Twombly*, 550 U.S. at 557). Ultimately, the court in *Legg* concluded that the plaintiff’s allegations, at best, “lead to a plausible inference that at some unknown time in the future, some of the putative class members *may* be the victim of identity theft or fraud.” *Id.* at 994 (emphasis in original). However, this “non-imminent risk of possible future injury following [a] data breach” is not sufficient to confer standing. *Id.* (citing *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013)). The court further stated that “[g]iven the holding in *TransUnion*, it is far from clear that any case finding a concrete injury based merely on an abstract risk of future identity theft following a data breach is still good law.” *Id.* at 993.

In *McCombs v. Delta Grp. Elecs., Inc.*, the court denied standing to an employee who brought a putative class action against her employer following a data breach of the employer’s computer system, ruling that the plaintiff’s allegations of potential risks of harm were too speculative to confer standing. 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023). The *McCombs* court held that the possibility that the plaintiff’s “PII will be used by an unknown cybercriminal to potentially commit fraud or identity theft” was “premised on potential illegal activity yet to be committed (and which may never be committed) by an unknown third party.” *Id.* at 1072. These alleged injuries were too speculative to invoke the court’s jurisdiction. *Id.* (citing *Cooper v. Bonobos, Inc.*, No. 21-cv-854, 2022 WL 170622, at *1 (S.D.N.Y. Jan. 19, 2022) (dismissing claims arising from a data breach because “given the age and nature of the data, the risk of identity theft or fraud is too remote to constitute injury in fact”)). The *McCombs* court also agreed with the *Legg* court’s finding that increased spam communications following a data breach, without some supportive allegations, does not establish a causal link between the two. *Id.* at 1074 (citing *Legg*,

574 F. Supp. 3d at 993; *Blood v. LaBette County Med. Ctr.*, 5:22-cv-04036-HLT-KGG, 2022 WL 11745549, at *6 (D. Kansas Oct. 20, 2022) (unpublished) (reasoning “[t]he alleged inconvenient disruptions (such as spam calls, texts, and emails) do not constitute an injury in fact”); *Gordon v. Virtumundo, Inc.*, No. 06-0204, 2007 WL 145939, at *8 (W.D. Wash. May 15, 2007) (unpublished) (plaintiff lacked standing because the harm suffered “must rise beyond the level typically experienced by consumers—i.e., beyond the annoyance of spam”); *Travis v. Assured Imaging LLC*, 20-CV-00390, 2021 WL 1862446, at *2 (D. Ariz. May 10, 2021) (unpublished) (holding “a dramatic increase in targeted spam phone calls after the ransomware attack” did not constitute an injury for standing purposes); *Cooper v. Bonobos*, 21-CV-854 (JMF), 2022 WL 170622, at *16 (S.D.N.Y. Jan. 19, 2022) (unpublished) (finding no injury in fact where plaintiff did not demonstrate that spam texts, calls, and e-mails were “fairly traceable” to the data breach).

In *Masterson v. IMA Fin. Grp., Inc.*, even when a plaintiff alleged that he suffered misuse of his PII when unauthorized charges appeared on a Medicare explanation of benefits or credit card, the court still found no standing when “[t]he only link between the data breach and the claimed misuse [was] that the misuse came after the data breach.” 2:23-cv-02223-HLT-ADM, 2023 WL 8647157, at *4 (D. Kansas Dec. 14, 2023) (unpublished). The *Masterson* court determined that such allegations did “not allege a ‘substantial likelihood’ that the data breach caused the misuse.” *Id.* (citing *Blood*, 2022 WL 11745549, at *5 (noting that the plaintiffs “do not plead any facts suggesting how the mere possession of their Social Security numbers and names would enable someone to make unauthorized charges on an existing account (instead of, for example, opening a new account)”); *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. 2015) (“Plaintiff’s allegations that someone attempted to open a bank account in his name,

attempted to log in to his email accounts, and that he received an increased number of email advertisements targeting his medical conditions do not allege injuries in fact fairly traceable to the Data Breach, since Plaintiff has not alleged that bank account information or email addresses were on the stolen backup data tapes.”).

In *Deevers Stoichev v. Wing Fin. Servs. LLC*, the court noted that, “[w]hile the Tenth Circuit has yet to consider the issue, many circuits have assessed whether plaintiffs have standing when they receive notice that their data may have been subject to a data breach, but have not faced actual harm.” 22-CV-0550-CVE-JFJ, 2023 WL 6133181, at *5 (N.D. Okla. Sept. 19, 2023) (citing cases) (unpublished). The court noted that the various circuits “have relied on a variety of non-dispositive factors to determine whether an alleged future risk of identity theft is imminent, including but not limited to, ascertaining (1) whether the data breach was intentionally targeted, (2) whether the data was misused, and (3) whether the data accessed was of a particularly sensitive nature.” *Id.* Applying these factors, the court found that the plaintiffs and the putative class did “not establish[] standing based on an increased and imminent risk of identity theft, fraud, or misuse.” *Id.*

Under all of these authorities, Plaintiff here has not, and cannot, establish a concrete injury as required by law to establish the requisite standing.

C. Plaintiff Has Not Alleged a Concrete Injury as a Result of the Incident and Instead Alleges a Host of Conjectural Future Injuries.

Plaintiff has alleged that “[a]s a result of the Data Breach, [she] is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.” Compl. ¶ 144. Plaintiff anticipates “spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach” “including researching and verifying the legitimacy

of the Data Breach, researching online how to protect herself from fraud and identity theft, . . . and monitoring her financial accounts for any indication of fraudulent activity” despite already signing up for the 12-month credit monitoring Defendant offered.³ *Id.* ¶¶ 139, 143. Plaintiff claims that the Data Breach “caused [her] to suffer fear, anxiety, and stress” that compounds from not knowing “key details about the Data Breach’s occurrence.” *Id.* ¶ 142. However, all of these categories of harm have been rejected. *Clapper*, 568 U.S. at 416 (Plaintiff “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.”); *see also Legg*, 574 F. Supp. 3d at 994; *Masterson*, 2023 WL 8647157 at *7. Further, “[i]t is well established that plaintiffs ‘cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.’” *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021) (quoting *Clapper*, 568 U.S. at 416). In the data breach context, Plaintiff’s efforts to mitigate the risk of future harm are not any more sufficient to confer standing than the risk of harm alone because the mitigation efforts are “inextricably tied to his perception of the actual risk of identity theft.” *Id.*; *see also In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (“Because plaintiffs

³ It would be unreasonable and inequitable to find that Plaintiff has suffered injury by incurring credit monitoring fees, report fees, and freeze fees, despite AMC having offered her a free 12-month subscription to credit monitoring services. Holding otherwise would harm consumers because companies will refuse to provide credit monitoring services, in the aftermath of a data breach, for fear of opening themselves up to lawsuits. *See Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir. 2017) (“To adopt such a presumption would surely discourage organizations from offering these services . . . lest their extension of goodwill render them subject to suit.”); *see also Clapper*, 568 U.S. at 409, 416 (noting that plaintiffs may not “manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is certainly not impending”).

have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury”); *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 571 (D. Md. 2016) (“In the context of data breach litigation, courts have consistently held that a plaintiff may not use mitigation costs alone to establish a cognizable injury in fact.”). Plaintiffs may not bootstrap one speculative injury to another to confer standing on themselves.

Plaintiff’s diminution-of-value theory fares no better. For example, in *Chambliss v. Carefirst, Inc.*, the case involved a data breach of CareFirst, a health insurance provider, that compromised individuals’ data including “the names, birth dates, email addresses, and subscriber identification numbers of the affected individuals.” 189 F. Supp. 3d at 567. The *Chambliss* court held that it “need not decide whether such personal information has a monetary value, as Plaintiffs have not alleged that they have attempted to sell their personal information or that, if they have, the data breach forced them to accept a decreased price for that information.” *Id.* at 572. Likewise, Plaintiff here has not alleged that she attempted to sell her data and sustained a loss in value attributable to the data incident at AMC.

Similarly, in *Khan v. Children’s Nat’l Health Systems*, the court rejected plaintiffs’ allegations that they suffered loss of value in their personal identifying information. 188 F. Supp. 3d 524, 533–34 (D. Md. 2016). That case involved a data breach at a hospital that compromised patient information including “names, addresses, dates of birth, Social Security numbers, and telephone numbers, as well as private health care information.” *Id.* at 527. The court rejected the plaintiff’s damages theory because the plaintiff did not “explain how the hackers’ possession of that information ha[d] diminished its value, nor d[id] she assert that she would ever actually sell

her own personal information.” *Id.* at 533. Likewise, Plaintiff here has not alleged how the value in her property has dropped or that she would ever actually sell her data.

Significantly, Plaintiff does not allege that any of her PII has been placed on the dark web, nor does she allege any financial harm based on fraud or theft resulting from the Incident. Ultimately, in accordance with *TransUnion*, the risk of unmaterialized future harm to Plaintiff is not concrete harm that can confer standing to her. Accordingly, all of Plaintiff’s claims must be dismissed pursuant to Rule 12(b)(1).

II. EVEN IF PLAINTIFF HAD STANDING, PLAINTIFF HAS FAILED TO STATE A CAUSE OF ACTION.

As established above, Plaintiff lacks standing to bring this suit and her claims must be dismissed in their entirety pursuant to Rule 12(b)(1). But even if Plaintiff did have standing to bring her claims, Plaintiff’s Complaint must be dismissed as she fails to state a cause of action.

A. The Court Should Dismiss Plaintiff’s Negligence Claims (in Counts I and II) Because They Are Based on Damages Arising From Future Harm.

Unlike some jurisdictions, Utah courts have not recognized a cause of action for present damages based on future harm in the data breach context. Utah does recognize no-injury medical monitoring, but only as a remedy for negligent exposure to hazardous substances. *See Hansen v. Mountain Fuel Supply Co.*, 858 P.2d 970, 979 (Utah 1993). *Hansen* permitted an independent cause of action for medical monitoring, but only when a plaintiff can prove exposure to a “toxic substance” caused by the defendant’s negligence that produced an increased risk of illness for which a medical test allowing early detection exists. *Id.* As is clear, this is a very narrow cause of action that does not extend to data breach cases or the types of injuries Plaintiff alleges here. Instead, a cause of action requires a present injury. *See, e.g., Gonzalez v. Russell Sorensen Const.*,

2012 UT App 154, ¶ 20, 279 P.3d 422 (finding the traditional elements of a claim of negligence must include “that the plaintiff in fact suffered injuries or damages”). Even were Plaintiff to have standing to bring these claims—which she does not—she lacks a legal basis to pursue present damages for future harms. At a minimum, Counts I and II should be limited to claims for mitigation or out-of-pocket expenses. Plaintiff’s claims for the value of future risk should be dismissed.

B. The Court Should Dismiss Plaintiff’s Negligence Claims Because They are Barred by the Economic Loss Rule.

In addition to Plaintiff’s negligence claims being barred based on future harm, Plaintiff’s claims for mitigation damages also fail under the economic loss rule. To recover on a claim for negligence in Utah, “the plaintiff must establish four essential elements: (1) that the defendant owed the plaintiff a duty, (2) that the defendant breached that duty, (3) that the breach of duty was the proximate cause of the plaintiff’s injury, and (4) that the plaintiff in fact suffered injuries or damages.” *Id.* However, even if a plaintiff can prove those elements, the economic loss rule prevents a plaintiff’s recovery in tort for damages of a purely economic nature. *Reighard v. Yates*, 2012 UT 45, ¶ 14, 285 P.3d 1168. The economic loss rule “marks the fundamental boundary between contract law, which protects expectancy interests created through agreement between the parties, and tort law, which protects individuals and their property from physical harm by imposing a duty of reasonable care.” *Id.* ¶ 19 (quoting *Davencourt at Pilgrims Landing Homeowner’s Ass’n v. Davencourt at Pilgrims Landing, LC*, 2009 UT 65, ¶ 18). Losses covered by the economic loss rule include:

[d]amages for inadequate value, costs of repair and replacement of the defective product, or consequent loss of profits—without any claim of personal injury or damage to other property . . . as well as the diminution in the value of the product because it is inferior in

quality and does not work for the general purposes for which it was manufactured and sold.

Id. ¶ 20 (alterations in original) (quoting *Am. Towers Owners Ass’n, Inc. v. CCI Mech., Inc.*, 930 P.2d 1182, 1189 (Utah 1996), *abrogated on other grounds by Davencourt*, 2009 UT 65, ¶ 55). “Under such circumstances, the contract is the exclusive means of obtaining economic recovery.” *Id.* “Whether the economic loss rule applies depends on ‘whether a duty exists independent of any contractual obligations between the parties.’” *Id.* ¶ 21.

Thus, even if Plaintiff had Article III standing, her negligence claims are barred by the economic loss doctrine because the only cognizable injury she has alleged is financial loss, which, if viable, can be redressed by her implied contract theory. *Id.* (“[O]nce there is a contract, any tort claim must be premised upon an independent duty that exists apart from the contract. All contract duties, and all breaches of those duties . . . must be enforced pursuant to contract law.”) (second alteration in original) (quoting *Grynberg v. Questar Pipeline Company*, 2003 UT 8, ¶ 43)). Plaintiff’s complaint alleges purely economic losses, and Plaintiff, therefore, cannot state a negligence or negligence *per se* claim under Utah law. *Id.* ¶¶ 19-22. The Court should therefore dismiss Counts I and II.

C. The Court Should Dismiss Plaintiff’s Negligence Claims in Counts I and II Because AMC Did Not Owe a Duty to Protect her From Unforeseeable Hacks into AMC’s System.

The duty of care owed under Utah law is “the degree of care which a reasonable person would have exercised under the same circumstances.” *Barson v. E.R. Squibb & Sons*, 682 P.2d 832, 835 (Utah 1984). In Utah, while there is a duty to protect business invitees “from criminal acts by third parties,” “the duty does not arise until the business owner knows, or should know, that criminal acts are likely to occur.” *Steffensen v. Smith’s Mgmt. Corp.*, 862 P.2d 1342, 1344-45

(Utah 1993). Otherwise, the crime is not foreseeable as a matter of law. *See id.* Plaintiff has not alleged any facts that would allow the Court to conclude AMC either knew or had reason to know that its data system was susceptible or at risk to third party criminals. As such, the Court should dismiss Counts I and II for this reason as well.

To allege a claim of negligence based on a data breach, a plaintiff must plausibly allege the breach *and* that the defendant caused the breach by failing to reasonably protect the subject data. *See, e.g., In re Waste Mgt. Data Breach Litig.*, 2022 WL 561734, at *5 (S.D.N.Y. Feb. 24, 2022) (“*Waste Mgt.*”) (unpublished) (beyond pleading a data breach, the plaintiff must plausibly allege “the breach was caused by [defendant’s] unreasonable conduct”). Here, Plaintiff has not sufficiently alleged the absence of reasonableness.

In *Waste Mgt.*, the Southern District of New York evaluated a negligence claim arising from a data breach, brought by current and former employees against USA Waste-Management (“Waste Management”) based on a cyber-attack that may have compromised employee PII. *Id.* at *1. The plaintiffs’ complaint included “many conclusory allegations that Waste Management failed to take reasonable measures to protect its data,” but pled “no facts regarding any specific measures that Waste Management did or didn’t take, nor [did] it contain any allegations regarding the manner in which their systems were breached.” *Id.* at *4. In essence, the complaint sought to “hold Waste Management liable for the fact of the data breach alone.” *Id.* at *5. That allegation was insufficient to save the negligence claim. *Id.*

Here, Plaintiff alleges AMC had a duty of care to “use reasonable means to secure and safeguard their computer property—and Class Members’ PII held within it—to prevent disclosure of the information, and to safeguard the information from theft.” *Id.* ¶ 167. These allegations,

however, do not provide sufficient information from which it can be inferred that AMC acted unreasonably in protecting data on its system. A duty to take reasonable steps to protect data from cyberattacks is very different than a duty to absolutely prevent those attacks from happening. Plaintiff does not identify what was unreasonable about AMC's data system. Such conclusory allegations do not merit the Court's consideration. *Twombly* 550 U.S. at 555 ("[O]n a motion to dismiss, courts 'are not bound to accept as true a legal conclusion couched as a factual allegation.'" (citation omitted)). The Complaint does not contend what measures, or combination of measures among any of the vague assertions identified AMC "should" have implemented to create a "reasonable" data security system. The Complaint does not allege what measures AMC "failed" to use in its data security system, nor how the use of any such measures would have elevated AMC's supposedly inadequate security system to a reasonable one.

Plaintiff's accusations of unreasonable conduct boil down to a litany of unsupported conclusory statements stemming from the notion that the "occurrence of the Data Breach indicates" AMC did not operate a reasonably adequate data security system. Compl. ¶ 41. Yet *Waste Mgt.* teaches the "fact of the data breach alone" is insufficient to infer unreasonable conduct by the party seeking to protect data. 2022 WL 561734, at *5. Without a plausible allegation that AMC failed to take reasonable measures to protect the PII in its possession, Plaintiff fails to sufficiently allege AMC acted unreasonably in attempting to protect Plaintiff's PII. Accordingly, Counts I and II should be dismissed for lack of duty.

D. The Court Should Dismiss Plaintiff's Negligence *Per Se* Claim in Count II Because Plaintiff Has Not and Cannot Specify a Standard of Care in the FTC Act that Was Violated or Which Constitutes Negligence *Per Se*.

Plaintiff's negligence *per se* claim, which is based on Section 5 of the FTC Act, must also be dismissed because the FTC Act does not provide any private right of action. *Drake v. Sometime Spouse, LLC*, 784 F. App'x 602, 604 (10th Cir. 2019) (citing *Am. Airlines v. Christensen*, 967 F.2d 410, 414 (10th Cir. 1992)).

Moreover, in Utah, before violation of a legislative standard will be held to be negligence *per se*, or prima facie evidence of negligence, the legislative standard must first be adopted by the court as defining the standard of conduct of a reasonable person. *Colosimo v. Gateway Community Church*, 2018 UT 26, ¶ 45, 424 P.3d 866. "In other words, before a statute or ordinance 'can be used as a basis for imposing a tort duty . . . , [the court] must be persuaded that the *purpose* of the statute [or ordinance] was to protect a class of persons of which [the plaintiff in the case] is a member and to protect [such plaintiff] against injury or death resulting from' the kind of harm contemplated by the legislature." *Id.* (emphasis and alterations in original) (quoting *Rollins v. Petersen*, 813 P.2d 1156, 1163 (Utah 1991), *overruled on other grounds by Scott v. Universal Sales, Inc.*, 2015 UT 64). "[T]he plaintiff bears the burden of showing that the ordinance was *intended* to protect persons in the plaintiff's shoes from the type of harm that befell the plaintiff." *Id.* (emphasis in original).

AMC is unaware of any case where Utah law has specifically allowed a cause of action based on a negligence *per se* theory arising from Section 5 of the FTC Act. If no such case exists, then this Court must "endeavor to predict" whether the Utah Supreme Court would adopt Section 5 of the FTC Act as imposing a duty recognizable in tort. *See Mitchell*, 355 F. Supp. 3d at 1157.

In *Mitchell*, plaintiffs attempted to assert a claim for negligence per se on the theory that the defendant violated the Gramm-Leach-Bliley Act (“GLBA”) by not adequately safeguarding plaintiffs’ sensitive personal information. *Id.* at 1156. The Utah District Court noted plaintiffs had not identified a Utah case adopting the GLBA as imposing a duty in tort. *Id.* at 1157. The court then held the Utah Supreme Court would likely not adopt the GLBA as imposing a duty recognizable in tort because no Utah court had ever established a state-law tort duty arising out of a federal statute that “lacked a private right of action.” *Id.* at 1158. Further, in Utah, only the violation of a statute involving dangerous instrumentalities constitutes negligence per se. *Id.*

Because Section 5 of the FTC Act does not allow a private right of action and does not deal with dangerous instrumentalities, the Utah Supreme Court likely would hold an FTC Act violation could not support a negligence per se claim. Therefore, Plaintiff’s negligence *per se* claim (“Count II”) must be dismissed.⁴

E. The Court Should Dismiss Plaintiff’s Breach of Implied Contract Claim in Count III Because Plaintiff Fails to Allege Any Material Terms and Conditions Sufficient to Sustain her Claim.

The elements of a prima facie case for breach of contract are (1) a contract, (2) performance by the party seeking recovery, (3) breach of the contract by the other party, and (4) damages. *Syme v. Symphony Group LLC*, 2018 UT App 212, ¶ 23, 437 P.3d 576. “Whether a contract exists between parties is ordinarily a question of law.” *Id.* ¶ 13. In order for a binding contract to exist, it must “be shown that the parties had a meeting of the minds as to the integral features of the

⁴ Within the Tenth Circuit, the District of Colorado twice has held in data breach actions that plaintiffs could not recover under a theory of negligence per se based on alleged violations of the FTC Act under Colorado law. See *SELCO Community Credit Union v. Noodles & Co.*, 267 F. Supp. 3d 1288, 1297, n 4 (D. Colo. 2017); *Bellwether Community Credit Union v. Chipotle Mexican Grill*, 353 F. Supp. 3d 1070, 1085-1086 (D. Colo. 2018).

agreement and that the terms are sufficiently definite as to be capable of being enforced.” *Id.* “A contract implied in fact is a ‘contract’ established by conduct.” *Davies v. Olson*, 746 P.2d 264, 269 (Utah Ct. App. 1987). “The elements of a contract implied in fact are (1) the defendant requested the plaintiff to perform work; (2) the plaintiff expected the defendant to compensate her for those services; and (3) the defendant knew or should have known that the plaintiff expected compensation.” *Id.*

Here, Plaintiff fails to meet this standard. Plaintiff alleges that an implied contract was formed merely because Plaintiff provided her PII to AMC, thereby obligating AMC to reasonably safeguard Plaintiff’s PII. Compl. ¶ 208. However, this barebone recital is the full extent of Plaintiff’s allegations regarding the formation of an implied contract and does not support any claim for breach of an implied agreement.

Courts in other data breach cases “have consistently held that the fact that a defendant required plaintiffs to provide personal information does not alone support the inference that the parties agreed for the defendant to secure this information.” *In re Am. Med. Collection Agency Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *19-20 (D.N.J. Dec. 16, 2021) (unpublished) (dismissing plaintiffs’ claim for breach of implied contract where plaintiffs paid defendants to perform healthcare services and defendants incidentally required personal information to ensure they received payment through plaintiffs’ insurers). Because Plaintiff’s allegations fail to state a claim for breach of implied contract, the Court should dismiss Plaintiff’s implied contract claim (Count III).

F. The Court Should Dismiss Plaintiff's Invasion of Privacy Claim in Count IV Because Plaintiff Has Not Alleged AMC Committed Intentional or Highly Offensive Conduct.

Under Utah law, “in order to establish a claim of intrusion upon seclusion, the plaintiff must prove two elements by a preponderance of the evidence: (1) that there was ‘an intentional substantial intrusion, physically or otherwise, upon the solitude or seclusion of the complaining party,’ and (2) that the intrusion ‘would be highly offensive to the reasonable person.’” *Stien v. Marriott Ownership Resorts, Inc.*, 944 P.2d 374, 378 (Utah Ct. App. 1997) (citation omitted). For example, the type of conduct that would support a claim includes “eavesdropping upon private conversations by means of wiretapping and microphones,” “peering into the windows of a home, and persistent and unwanted telephone calls.” *Id.* (quoting W. Page Keeton et al., *Prosser and Keeton on the Law of Torts* § 117, at 854-55 (5th ed. 1984)).

Plaintiff fails to allege the required elements to support an intrusion of Plaintiff's privacy. Plaintiff alleges only that AMC failed to avoid the disclosure of Plaintiff's PII by allowing unauthorized parties to unauthorizedly use said information. However, Plaintiff does not allege any intentional act by AMC to intrude into Plaintiff's private matters. *See Stien*, 944 P.2d at 378 (intentional conduct requires intrusion upon physical solitude, or a person prying into another's private affairs, such as opening another person's mail); *Schmitt v. SN Servicing Corp.*, No. 21-cv-03355-WHO, 2021 WL 5279822, at *3-4 (N.D. Cal. Nov. 12, 2021) (dismissing invasion claim because “procuring information via security breach is “inherently different than obtaining it through an agreed-upon exchange” and noting intentional disclosures to be a “far cry from the allegations at hand,” which contained “no indication of any intentional sharing of information”).

Further, there is no conduct on the part of AMC that in any way could be construed to be “highly offensive to the reasonable person.” *Stien*, 944 P.2d at 378. Plaintiff alleges only that AMC had inadequate information security practices. Compl. ¶ 228. However, inadequate security is not highly offensive conduct. *See, e.g., Razuki v. Caliber Home Loans, Inc.*, No. 17cv1718-LAB (WVG), WL 2761818, at *2 (S.D. Cal. June 8, 2018) (allegations that defendant implemented “low-budget security measures” with “disregard of [the] consequences” were inadequate to state invasion claim); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (“[N]egligent conduct that leads to theft of highly personal information, including social security numbers, does not ‘approach [the] standard’ of actionable conduct . . . and thus does not constitute a violation of Plaintiffs’ right to privacy.” (citation omitted)). For these reasons, the Court should dismiss Count IV.

G. The Court Should Dismiss Plaintiff’s Unjust Enrichment Claim in Count V Because Plaintiff Does Not Allege How AMC Benefited From Receiving her Private Information.

Plaintiff’s unjust enrichment claim fails because Plaintiff has not alleged any benefit to AMC. Under Utah law, to prevail on a claim for unjust enrichment, “a plaintiff must show: (1) a benefit conferred; (2) an appreciation or knowledge by the conferee of the benefit; and (3) the acceptance or retention of the benefit by the conferee under such circumstances as to make it inequitable for the conferee to retain the benefit without payment of its value.” *U.S. Fid. v. US Sports Specialty*, 2012 UT 3, ¶ 12, 270 P.3d 464 (internal citations omitted) (cleaned up). While some courts have recognized that victims of a data breach may be able to state a claim for unjust enrichment “in situations where businesses commoditize or receive an independent pecuniary

benefit from holding the Personal Information,” *In re American Medical*, 2021 WL 5937742, at *18, that is not the case here.

Plaintiff has failed to allege how a benefit was conferred on AMC from receiving Plaintiff’s PII. The Complaint contains only a conclusory statement that AMC benefited from the receipt of Plaintiff’s and the Class’s PII, while Plaintiff and the Class should have had their PII protected with adequate data security. Compl. ¶ 236. However, this is insufficient to show that AMC “unjustly retained” a benefit at Plaintiff’s expense. For example, Plaintiff does not allege that AMC failed to provide the service for which she paid. *See Gokool v. Oklahoma City Univ.*, 716 F. App’x 815, 819 (10th Cir. 2017) (affirming dismissal of unjust enrichment claim where student paid tuition and in exchange received the instruction the school agreed to provide). Moreover, Plaintiff does not allege that AMC received any independent pecuniary benefit from the retention of Plaintiff’s PII. Therefore, Plaintiff’s unjust enrichment claim (Count V) should be dismissed.

CONCLUSION

For the reasons set forth above, AMC respectfully requests that this Court grant its Motion to Dismiss Plaintiff’s Complaint in its entirety.

DATED this 1st day of May 2024.

RAY QUINNEY & NEBEKER P.C.

/s/ Kamie F. Brown
Kamie F. Brown
Kristina M. DuBois

Justin J. Boron (*pro hac vice forthcoming*)
Kevin M. Ringel (*pro hac vice forthcoming*)
FREEMAN MATHIS & GARY, LLP

Attorneys for Academy Mortgage Corporation